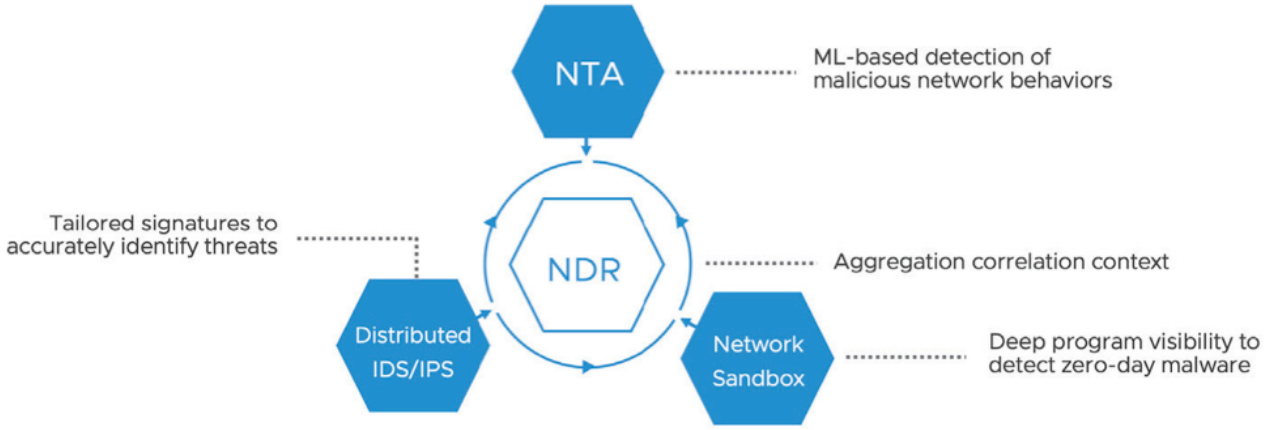
Exhibit 7

CHART FOR U.S. PATENT NO. 9,264,441 ("the '441 Patent")

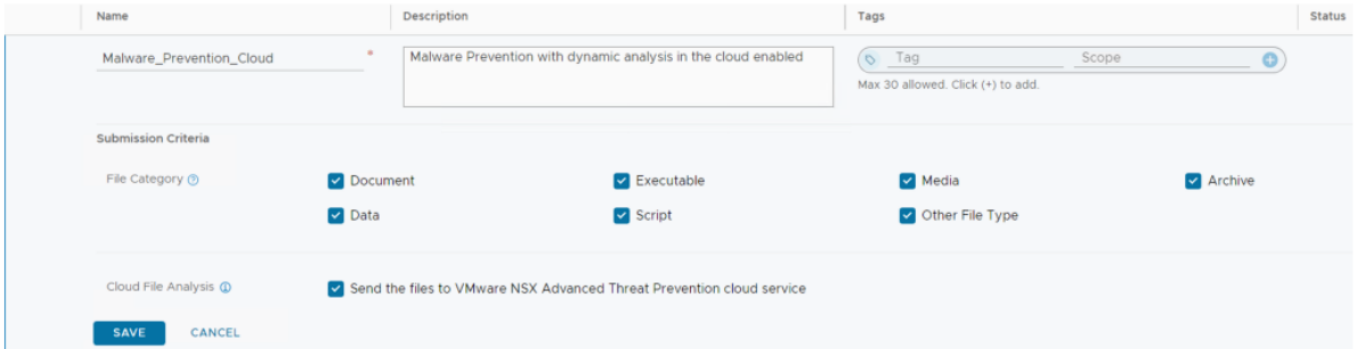
Accused Products: VMware's products, including at least each of the following appliances and software infringe at least Claim 11 of the '441 Patent: NSX Distributed Firewall with Advanced Threat Prevention, NSX Gateway Firewall with Advanced Threat Prevention, NSX Advanced Threat Prevention (standalone). The infringement chart below is based on the NSX Gateway Firewall with Advanced Threat Prevention ("NSX Advanced Threat Prevention"), which is exemplary of the infringement of the '441 Patent by all of the Accused Products.

Claims	Exemplary Infringement Evidence
[11pre] A non-transitory machine-readable medium comprising machine readable instructions that when executed by a processor perform a method, the machine readable instructions to cause the processor to:	To the extent the preamble is limiting, the Accused Products compris a non-transitory machine-readable medium comprising machine readable instructions that when executed by a processor perform a method, the machine readable instructions to cause the processor to perform the recited functions. To the extent the preamble is deemed limiting, NSX Advanced Threat Prevention comprises non-transitory machine-readable medium comprising machine readable instructions that when executed by a processor perform a method, the machine readable instructions to cause the processor to perform the recited functions. **The VMware Approach to Preventing Advanced Threats** VMware has taken an automated, distributed and enterprise-wide approach to preventing advanced threats. The solution, the VMware Advanced Threat Prevention (ATP) package, is an add-on to the VMware NSX Distributed Firewall [2]. ATP provides protection against advanced threats. It increases fidelity, reduces false positives, and accelerates remediation while simultaneously reducing the amount of manual work that analysts must do. *See* Advanced Threat Prevention with VMware NSX Distributed Firewall available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf at p. 2

Claims	Exemplary Infringement Evidence
	VMware's ATP incorporates multiple detection technologies and includes logic that combines information from all these (see Figure 1): • Detection technologies – Distributed IDS/IPS – Network sandbox – Network traffic analysis (NTA) • Network detection and response (NDR) – Aggregation, correlation, and context engines – Including the ability to pull context from sources outside NSX  **Figure 1:** ATP—multiple detection technologies + NDR *See* Advanced Threat Prevention with VMware NSX Distributed Firewall available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf at p. 3

Claims	Exemplary Infringement Evidence
	Network sandbox is a secure isolation environment that is designed to detect malicious artifacts in the data center. It analyzes the behavior of objects, such as files and URLs, to determine if they are benign or malicious. Because it is not reliant on signatures, the sandbox can detect novel and highly targeted malware that has never been seen before. VMware chose the most advanced method of sandboxing available: Full-system Emulation (FUSE)-based sandboxing [4]. *See* Advanced Threat Prevention with VMware NSX Distributed Firewall available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf at p. 3 VMware's sandbox implementation uses VMware Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices), to analyze malware. The sandbox continuously observes all the actions that a malicious object takes. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Claims	Exemplary Infringement Evidence
	Network Detection and Response is available across all three products in the NSX Security portfolio – • **NSX Distributed Firewall with Advanced Threat Prevention.** In this configuration, Network Detection and Response processes signals available across east-west network traffic and alerts security teams to potential lateral movement of threats. • **NSX Gateway Firewall with Advanced Threat Prevention.** In this configuration, Network Detection and Response processes traffic coming into or out of an environment and alerts security teams to infiltration and exfiltration attempts. VMware's Network Detection and Response implementation processes signals across both the Distributed and Gateway Firewall when these firewalls are deployed together. • **NSX Advanced Threat Prevention (standalone).** In this configuration, Network Detection and Response is deployed in an environment to protect non-vSphere workloads. Typically, neither the NSX Distributed Firewall nor the NSX Gateway Firewall is available in such environments. However, the Network Detection and Response functionality is similar to the other two configurations mentioned above. *See* Network Detection and Response available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-ndr-so.pdf at p. 2.
[11a] receive a plurality of packets destined for an internal operating system;	The Accused Products comprise machine readable instructions that cause the processor to receive a plurality of packets destined for an internal operating system. For example, NSX Advanced Threat Prevention receives a plurality of packets destined for an internal operating system.

Claims	Exemplary Infringement Evidence
	 *See* VMware NSX Advanced Threat Prevention NSX Malware Prevention can detect and prevent known malicious files and unknown malicious files. Unknown malicious files are also referred to as zero-day threats. To detect malware, NSX Malware Prevention uses a combination of the following techniques : • Hash-based detection of known malicious files • Local analysis of unknown files • Cloud analysis of unknown files *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED08F0.html

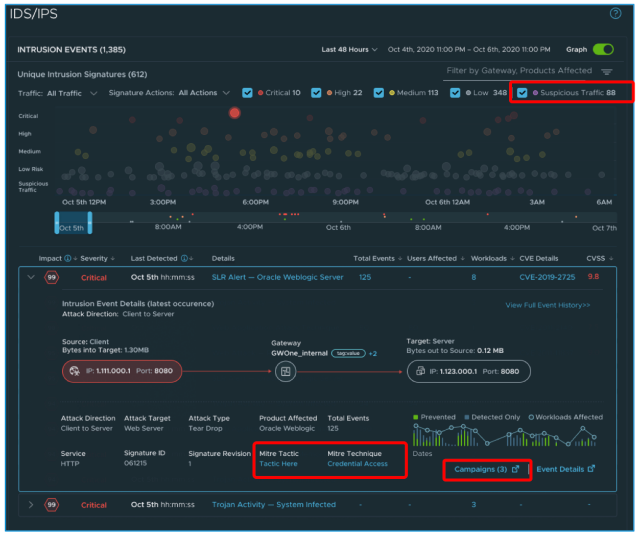
Claims	Exemplary Infringement Evidence
	## Cloud File Analysis Cloud file analysis is done by the NSX Advanced Threat Prevention service that is running in the cloud. It involves a detailed analysis of unknown files by using the following techniques to detect whether the file is benign, malicious, or suspicious: • NSX Malware Prevention sandboxing and behavioral analysis • Statistical algorithms • Artificial intelligence and machine learning • Deep content inspection NSX-T sends unknown files over a secure connection to the cloud only when you opt for cloud file analysis in your Malware Prevention security profile. ## File Event An event that is generated when a file is extracted or intercepted from the data path traffic on an NSX Edge or a Guest VM on the host. On an NSX Edge, the file is extracted by the NSX IDPS engine, and on a Guest VM, the file is extracted by the NSX File Introspection driver in the Guest Introspection (GI) thin agent. *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-BCC842E4-936A-49EE-B64E-CD90E915115D.html NSX Distributed IDS/IPS is an application-aware traffic inspection engine purpose built for analyzing internal East-West traffic and detecting lateral threat movements. The engine runs within the hypervisor to optimize packet inspection. NSX Distributed IDS/IPS combines industry-leading signature sets, protocol decoders and anomaly detection-based mechanisms to hunt for known and unknown attacks in the traffic flow. It also benefits from rich application context, driving lower false positive rates while incurring minimal computational overhead on the host. *See* https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-21-nsx-security-use-cases

Claims	Exemplary Infringement Evidence

A network sandbox intercepts artifacts entering and traversing the network.. The sandbox appears to the potential malware to be a fully-functioning end-user environment, and it coaxes suspicious files into running their routines — executing, downloading other files, connecting to URLs, etc. The sandbox analyzes a suspect file's and network behavior, and either allows the file to continue into the network, blocks it, or quarantines it for further investigation.

Network sandboxes are ideally combined with an advanced threat protection solution to round out detection and response capabilities.

See https://www.vmware.com/topics/glossary/content/network-sandbox.html



See NSX The Platform for Security available at https://www.vmware.com/content/dam/learn/en/emea/fy23/pdf/1245207_04-05-2022_NSX-Security-Platform.pdf at p. 5

Claims	Exemplary Infringement Evidence

Malware Prevention

Malware detection and Prevention for DFW (E-W)

Malware detection for GFW (N-S)

Known Malicious files and new Zero-days

Local (static) analysis and cloud-based dynamic analysis (sandbox detonation)

Guest-Introspection-based File extraction for DFW

IDPS based File extraction for GFW

Events logged locally and linked to Campaign via NDR

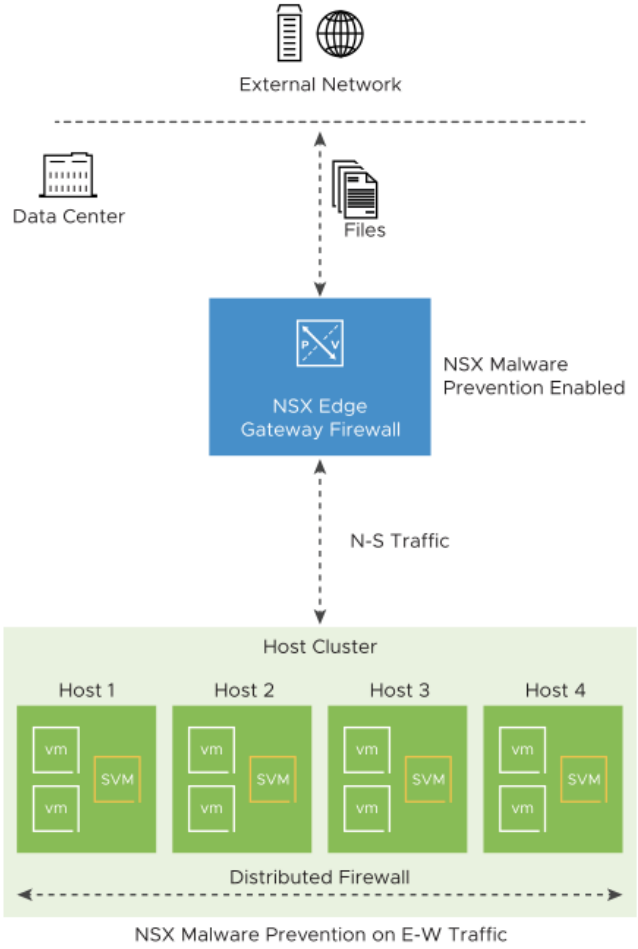
vmware

6

See NSX The Platform for Security available at https://www.vmware.com/content/dam/learn/en/emea/fy23/pdf/1245207_04-05-2022_NSX-Security-Platform.pdf at p. 6

> VMware's sandbox implementation uses VMware Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices), to analyze malware. The sandbox continuously observes all the actions that a malicious object takes.

Claims	Exemplary Infringement Evidence
	See Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1
[11b] store the plurality of packets in a buffer;	The Accused Products comprise machine readable instructions that cause the processor to store the plurality of packets in a buffer. For example, NSX Advanced Threat Prevention stores the plurality of packets in a buffer.

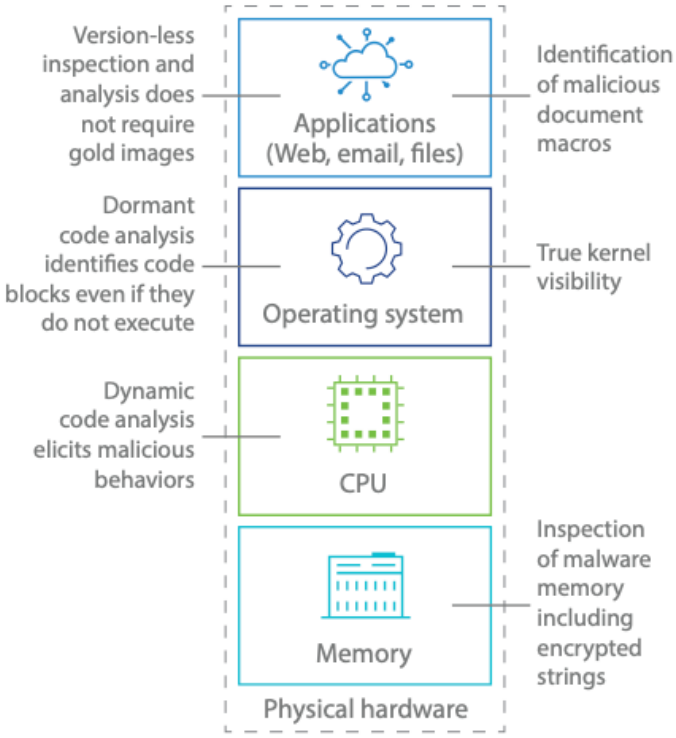
Claims	Exemplary Infringement Evidence
	 *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED08F0.html

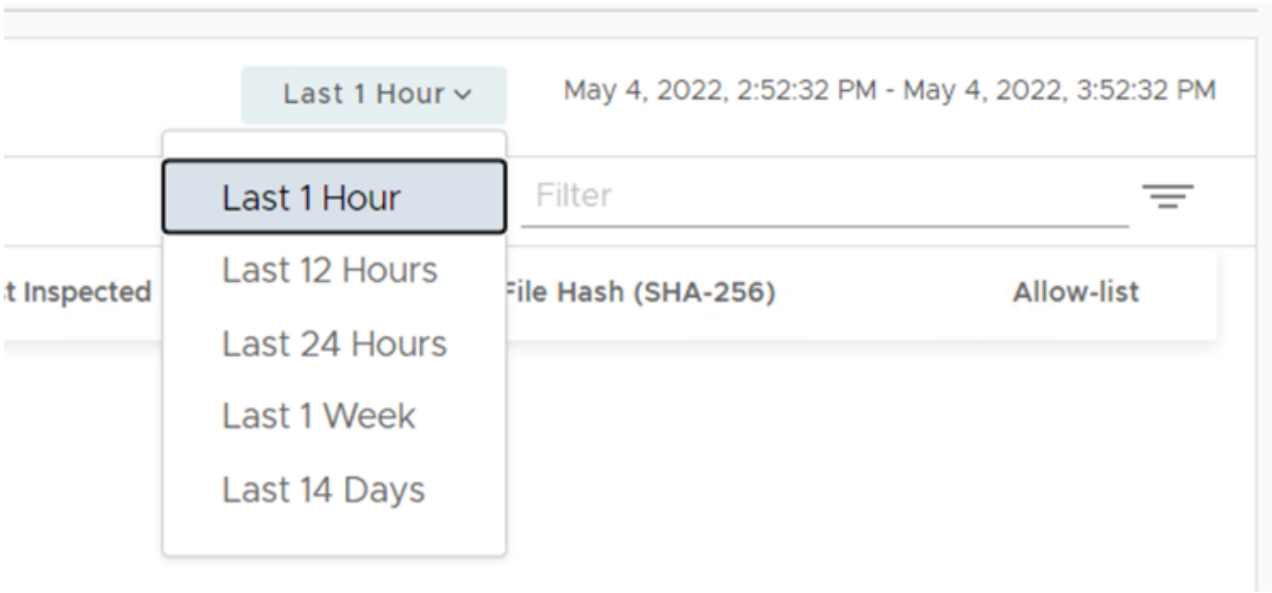
Claims	Exemplary Infringement Evidence
	On the north-south traffic, the NSX Malware Prevention feature uses the IDS/IPS engine on the NSX Edges to extract or intercept the files that are entering the data center. On the east-west traffic, this feature uses the capabilities of the NSX Guest Introspection (GI) platform. If the file bypasses scrutiny on the NSX Edge and reaches the host, the file is extracted by the GI thin agent on Windows guest VMs. To detect and prevent malware on Windows guest VMs, you must install the NSX Guest Introspection thin agent on Windows guest VMs, and deploy the NSX Distributed Malware Prevention service on vSphere host clusters that are prepared for NSX-T Data Center. When this service is deployed, a service virtual machine (SVM) is installed on each host of the vSphere cluster and NSX Malware Prevention is enabled on the host cluster. *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED08F0.html File events are generated when files are extracted by the IDS engine on the NSX Edges in the north-south traffic and by the NSX Guest Introspection agent on the virtual machine endpoints in the distributed east-west traffic. NSX Malware Prevention feature inspects the extracted files to determine whether they are benign, malicious, or suspicious. Each unique inspection of a file is counted as a single file event in NSX-T Data Center. In other words, a file event refers to a unique file inspection. For information about monitoring the NSX Malware Prevention file events by using the UI, see Monitoring File Events. *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED08F0.html File Event An event that is generated when a file is extracted or intercepted from the data path traffic on an NSX Edge or a Guest VM on the host. On an NSX Edge, the file is extracted by the NSX IDPS engine, and on a Guest VM, the file is extracted by the NSX File Introspection driver in the Guest Introspection (GI) thin agent. *See* https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-BCC842E4-936A-49EE-B64E-CD90E915115D.html

Claims	Exemplary Infringement Evidence
[11c] forward a copy of each packet of said plurality of packets to a virtual machine emulating said internal operating system;	The Accused Products comprise machine readable instructions that cause the processor to forward a copy of each packet of said plurality of packets to a virtual machine emulating said internal operating system. For example, NSX Advanced Threat Prevention forwards a copy of each packet of said plurality of packets to a virtual machine emulating said internal operating system.  Malware Prevention Malware detection and Prevention for DFW (E-W) Malware detection for GFW (N-S) Known Malicious files and new Zero-days Local (static) analysis and cloud-based dynamic analysis (sandbox detonation) Guest-Introspection-based File extraction for DFW IDPS based File extraction for GFW Events logged locally and linked to Campaign via NDR vmware 6 *See* NSX The Platform for Security available at https://www.vmware.com/content/dam/learn/en/emea/fy23/pdf/1245207_04-05-2022_NSX-Security-Platform.pdf at p. 6

Claims	Exemplary Infringement Evidence
	The Engine uses Deep Content Inspection, a unique isolation and inspection environment (sandbox) that simulates an entire host (including the CPU, system memory, and all peripherals) and its operating environment to analyze potentially malicious files. Unknown files, such as applications and documents, and URLs, are submitted from the Manager and other sources. The Engine runs these artifacts in its sandbox and returns the results of its analysis to the Manager, which then displays results. *See* Engine Installation and Administration available at https://docs.vmware.com/en/VMware-NSX-Network-Detection-and-Response/9.7/Engine_Installation_Manual_9.7.pdf at p. 1 With a network sandbox, security teams can carry out advanced malware analysis by allowing suspicious files to run in a segregated environment that emulates an actual end-user operating environment. *See* https://www.vmware.com/topics/glossary/content/network-sandbox.html VMware's sandbox implementation uses VMware Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices), to analyze malware. The sandbox continuously observes all the actions that a malicious object takes. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1
[11d] monitor performance of said virtual machine in processing the forwarded packets;	The Accused Products comprise machine readable instructions that cause the processor to monitor performance of said virtual machine in processing the forwarded packets. For example, NSX Advanced Threat Prevention monitors performance of said virtual machine in processing the forwarded packets.

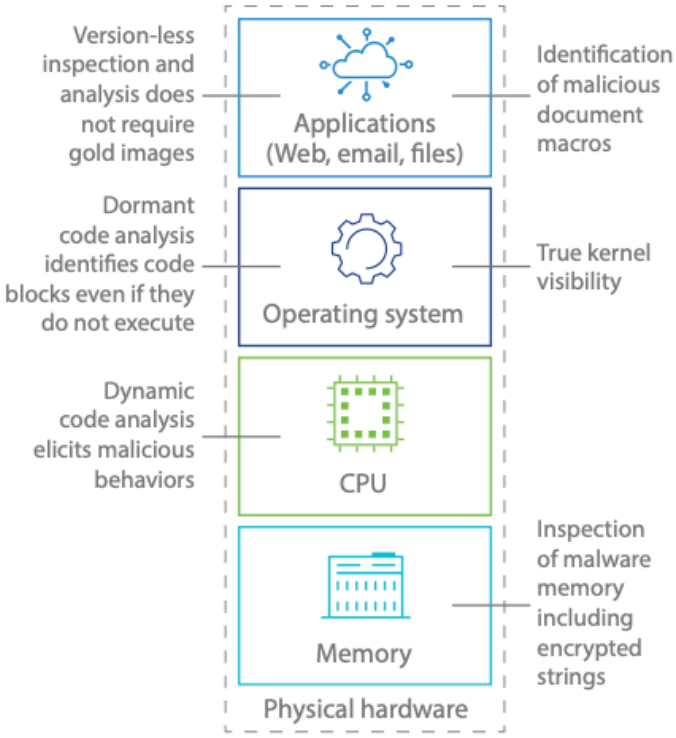
Claims	Exemplary Infringement Evidence
	Further, the sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, the sandbox identifies the memory (RAM) locations accessed by the artifact being analyzed. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Claims	Exemplary Infringement Evidence
	 **Figure 2:** VMware Deep Content Inspection delivers unmatched visibility *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 2
[11e] delete a packet of the plurality of packets from the buffer upon	The Accused Products comprise machine readable instructions that cause the processor to delete a packet of the plurality of packets from the buffer upon a determination that said packet was stored in the buffer for a predetermined time period.

Claims	Exemplary Infringement Evidence
a determination that said packet was stored in the buffer for a predetermined time period;	For example, NSX Advanced Threat Prevention deletes a packet of the plurality of packets from the buffer upon a determination that said packet was stored in the buffer for a predetermined time period.  *See* NSX Malware Prevention Dashboard You can monitor events and view data of the last 14 days. To view intrusion events, navigate to **Security > IDS/IPS** . You can filter the events based on the following criteria: *See* https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-852AADD3-653F-4C1C-A10E-24D03B4084CA.html

Claims	Exemplary Infringement Evidence
[11f] detect a failure of said virtual machine; and	The Accused Products comprise machine readable instructions that cause the processor to detect a failure of said virtual machine. For example, NSX Advanced Threat Prevention detects a failure of said virtual machine. Further, the sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, the sandbox identifies the memory (RAM) locations accessed by the artifact being analyzed. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1 Full system emulation (FUSE) sandboxes emulate the entire hardware: CPU, memory, and I/O devices. The advantages are clear: it allows the sandbox to interact with the malware and conduct deep content inspection. This enables the sandbox to view everything the malware is doing, and lets analysts carefully study the malware and its operation. Because it emulates everything, it is much more difficult for cybercriminals to evade the sandbox. *See* Advanced Threat Prevention with VMware NSX Distributed Firewall available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf at p. 4
[11g] analyze said packets in said buffer and identify said malicious packet from said buffer	The Accused Products comprise machine readable instructions that cause the processor to analyze said packets in said buffer and identify said malicious packet from said buffer packets in response to detecting the failure of said virtual machine. For example, NSX Advanced Threat Prevention analyzes said packets in said buffer and identify said malicious packet from said buffer packets in response to detecting the failure of said virtual machine.

Claims	Exemplary Infringement Evidence
packets in response to detecting the failure of said virtual machine; and	Further, the sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, the sandbox identifies the memory (RAM) locations accessed by the artifact being analyzed. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Claims	Exemplary Infringement Evidence
	 **Figure 2:** VMware Deep Content Inspection delivers unmatched visibility *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 2

Claims	Exemplary Infringement Evidence

At a Glance

VMware's Network Sandbox provides advanced malware analysis of artifacts traversing your cloud environment. The sandbox deconstructs every behavior engineered into a file or URL and sees all instructions that a program executes, all memory content, and all operating system activity.

At VMware, Network Sandboxing is a component of NSX Advanced Threat Prevention along with Intrusion Detection/Prevention System (IDS/IPS), Network Traffic Analysis (NTA), and Network Detection and Response (NDR).

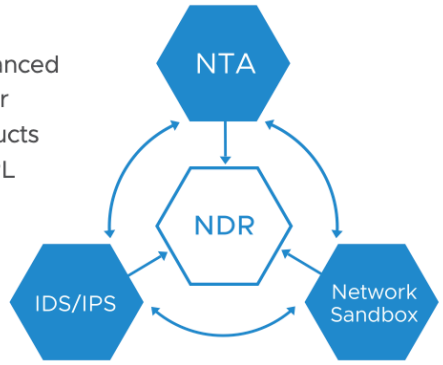


Figure 1: NSX Advanced Threat Prevention = IDS/IPS + Network Sandbox + NTA + NDR

See Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Further, the sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, the sandbox identifies the memory (RAM) locations accessed by the artifact being analyzed.

See Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Claims	Exemplary Infringement Evidence
	The sandbox's analysis of malicious artifacts provides you with the threat information you need for security workflows and policies. You receive both high-level, actionable threat intelligence and detailed host and network indicators of compromise (IoCs). *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1
[11h] create a malicious packet signature based upon the identified malicious packet.	The Accused Products comprise machine readable instructions that cause the processor to create a malicious packet signature based upon the identified malicious packet. For example, NSX Advanced Threat Prevention creates a malicious packet signature based upon the identified malicious packet. The sandbox's analysis of malicious artifacts provides you with the threat information you need for security workflows and policies. You receive both high-level, actionable threat intelligence and detailed host and network indicators of compromise (IoCs). *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 1

Claims	Exemplary Infringement Evidence
	The VMware Threat Analysis Unit™ automatically shares the malware characteristics, behaviors, and associated IoCs of every malicious object curated and analyzed by VMware with all VMware customers and partners. This allows for faster detection and analysis of previously unseen threats and reduces the time for you to respond to malicious activity. The sandbox also continuously updates the VMware Threat Analysis Unit in real time with intelligence from partner and customer environments worldwide. In addition, your threat analysts and incident response team can also subscribe to the VMware Threat Analysis Unit NSX knowledge base for faster response to previously known threats. The knowledge base contains the malware characteristics, behaviors, and associated IoCs of every malicious object curated and analyzed by the NSX team. *See* Network Sandbox available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf at p. 2